Expression of Interest (EOI)

1. **Subject:**
   Invitation of quotation rates from eligible bidders for performing Cyber Security Audit in BESCOM.

2. **Introduction and Background:**
   Power sector utilities are mandated to conduct periodic cybersecurity audit of both Information Technology (IT) and Operational Technology (OT) assets, through auditors empanelled by the CERT-In as per Article 14 of Central Electricity Authority (Cyber Security in Power Sector) Guidelines 2021.

   In order to adhere to the Guidelines, BESCOM needs to perform the Cyber Security Audit activity for all its IT/OT/IoT systems, web and mobile applications. BESCOM shall follow CSIRT-Power "Guidelines on Scope of Cybersecurity Audit in Power Sector" to perform the Cybersecurity audit. Some of the applications/systems are managed by BESCOM In-house and some are managed by service providers.

   Accordingly, this Expression of Interest (EOI) is being issued to discover the market price from eligible bidders to perform the Cyber Security audit activity in BESCOM.

   The CERT-In empanelled auditor needs to have domain specific expertise to assess IT, OT and IoT environments.

3. **Scope of work:**

   The scope under this requirement comprises two parts. Part 1 outlines guidelines for scope of cybersecurity audits to assess and validate BESCOMs overall cybersecurity postures, focusing on policies, processes, procedures, practices, governance structure and compliance with regulatory requirements. Part 2 defines the scope of Vulnerability assessment (VA) and Penetration Testing (PT) to address technical cybersecurity evaluations.

   The audit should adhere to applicable cybersecurity standards, such as ISO 27001, IS 16335, and the IEC 62443 series, and verify the BESCOMs cybersecurity resilience, including its compliance with applicable cybersecurity rules, regulations, directives, and guidelines.

   3.1 The objectives of the mandated Cybersecurity Audit:

   1. Comprehensive Coverage of Cyber Assets: The audit should ensure a thorough and comprehensive cybersecurity assessment of cyber assets within BESCOM, enabling the identification and mitigation of vulnerabilities.
   2. Assessment of IT, OT and IoT Architecture Resilience: It should assess the robustness of IT and/or OT and/or IoT architecture within the

BESCOMs interconnected environment.

3. Verification of Technical Controls and System Hardening: The audit should provide a structured evaluation of the effectiveness of implemented technical controls, hardening measures, and the configuration of security devices.
4. Assessment of Operational Technology (OT) Systems: The audit should include a comprehensive cybersecurity review of OT systems, considering the practical constraints inherent in OT environments.
5. Regulatory Compliance: The audit should enable BESCOM to verify compliance with applicable Acts, Rules, Regulation, Directives, and Guidelines issued by Government of India.
6. Gap Analysis Against Cybersecurity Frameworks: This audit should conduct a detailed gap analysis of BESCOMs cybersecurity practices in relation to the adopted cybersecurity frameworks, such as ISO 27001 for IT systems and IEC 62443-2-1 for OT systems, to guide ongoing improvements and enhance resilience.

3.2 Part 1- Guidelines for Scope of Comprehensive Cybersecurity Audit

The scope of the audit encompasses a systematic evaluation of Information Technology (IT), Operational Technology (OT), IoT systems, web and mobile applications within BESCOM, ensuring that all deployed cyber assets are included in the assessment. It should cover all critical components such as network infrastructure, security devices, technical controls, and system hardening measures, while also addressing the unique cybersecurity requirements of OT systems, which are vital to the power sector. The audit should further assess the effectiveness of existing security configurations and verify compliance with relevant cybersecurity frameworks and regulatory guidelines. Additionally, a detailed gap analysis should be conducted to identify areas for improvement, supporting the utility's ongoing cybersecurity enhancement efforts.

3.2.1 Systems, Assets, Policies, Processes & Procedures

The audit scope shall include, but not be limited to, the following:

1. all the identified Critical Information Infrastructures and notified Protected Systems of BESCOM,
2. all Critical and High-risk Assets as identified by BESCOM,
3. all medium and low-risk assets,
4. all web applications, mobile applications and cloud-based applications including APIs, internal applications as per risk based,
5. the utility's existing cybersecurity policies, processes, and procedures. This includes reviewing of the Service Level Agreements

(SLAs) with third-party vendors to ensure that SLA meets appropriate cybersecurity requirements,

6. the statement of applicability, selection, and implementation of cybersecurity controls,
7. review of the network architecture and data flow in IT, OT and IoT environments,
8. configuration assessment of deployed security devices,
9. vulnerability analysis of all notified protected systems and critical and high-risk assets, with medium and low-risk assets covered on a sample and rotational basis,
10. verification audit for compliance with applicable cybersecurity Rules, Regulations Directives and Guidelines issued by CERT-In, National Critical Information Infrastructure Protection Centre (NCIIPC), Central Electricity Authority (CEA) and other Government Entities.
11. review of the architecture at both main and backup control centers including their interconnections and data flow.
12. mechanism of Backup /Storage/DR Systems in place,
13. review of Cyber Crisis Management Plan of the utility and effectiveness of its implementation,
14. review of Emergency Preparedness Plan and Business Continuity Plan,
15. evaluation of physical security controls,
16. any additional system deemed suitable by BESCOM.

3.2.2 Detail of the Audit Areas:

Audit of the Cybersecurity Policy, Process and Procedure

1. Audit of Cybersecurity Policy Effectiveness and Alignment: The auditor will verify whether cybersecurity policy complies with latest edition of ISO 27001 and ISO 27019 standards, as applicable. This includes ensuring alignment with business goals, legal obligations, and contractual terms. Audit shall also verify the exceptions to ensure that these exceptions are authorized, legitimate and valid.
2. As applicable, audit of the OT specific cybersecurity policy, and its compliance with sector specific cybersecurity standards like IS 16335 and IEC 62443 series.
3. Audit of the cybersecurity governing structure such as designation of CISO with ring fenced cybersecurity duties, existence of dedicated

division for cybersecurity with defined roles & responsibilities and staffed with adequate and trained manpower.

4. Audit of the asset management process, and verification of the asset identification and classification process is in place.
5. Audit of the Vulnerability Management Process in both IT, OT and IoT systems, web and mobile applications for periodic identification and closure of vulnerabilities,
6. Audit of Risk Management Process to evaluate how BESCOM identifies, assesses, and manages cybersecurity risks.
7. Audit of the processes for managing changes to IT, OT and IoT systems, web and mobile applications and configurations. Audit of patch management procedures for applying patches to IT, OT and IoT systems, including pre-patch testing, post-patch validation, and rollback procedures.
8. Audit of the implemented process/mechanism for regular backups of critical operational and business data with tested recovery procedures and reports.
9. Audit of the personnel risk assessment process present with utility to mitigate internal and external cybersecurity risks from their own personnel or from that of their Service Provider having access to BESCOMs critical and high-risk assets
10. Audit of the process and procedure, in place for safe & secure disposal of legacy systems to verify that such systems are disposed as per established process.
11. Audit of the Supply Chain Risk Management system to evaluate their effectiveness in securing the supply chain and managing associated risks. This includes audit of the outsourced activities to mitigate risks from third-party vendors and their adherence to BESCOM cybersecurity policy and regulatory requirements.
12. Audit of existing cybersecurity training and awareness program to verify its suitability and adequacy. This includes assessment of user awareness w.r.t organization’s security policies, evaluation of the employee's susceptibility to social engineering attacks, such as phishing and impersonation.
13. Verification of the availability of a tailored and approved Cyber Crisis Management Plan (CCMP) that includes utility-specific cyber-attack scenarios and procedures, and assessment of whether the CCMP's efficacy is tested through mock drills and exercises.
14. Review of the business continuity and disaster recovery plans to ensure they are comprehensive and up to date.
15. Communications Security Testing- Evaluating the security measures implemented on communication channels to identify vulnerabilities and ensure that information transmitted over those

channels is protected from unauthorized access, interception, modification, or disruption.

16. Red Team Assessment- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems. Controlled and approved Red Team exercises limited to agreed scope and non-disruptive scenarios

17. Digital Forensic Readiness Assessment- Evaluating organization preparedness to effectively collect, preserve, and analyze digital evidence in the event of a security incident.

18. Industrial Control Systems/ Operational Technology Security Testing- Evaluating the cyber security posture of industrial control systems (ICS) and operational technology (OT) networks, specifically designed to identify vulnerabilities and potential threats that could disrupt critical industrial processes, impacting safety, production, and overall system availability within a facility.

19. Internet of Things (IOT)/ Industrial Internet of Things Security Testing (IIOT)-Evaluating and validating the security posture of connected devices within an IoT network, by identifying vulnerabilities and potential attack vectors.

20. Log Management and Maintenance Audit-Assessing the effectiveness and completeness of system and security log generation, retention, integrity, and monitoring practices, ensuring that logs are maintained in accordance with organizational policies and regulatory requirements to support detection, investigation, and response activities

21. Endpoint Security Assessment-Evaluating the security posture of endpoint devices (e.g., desktops, laptops, mobile devices) by assessing configurations, patching, malware protection, encryption, access controls, and monitoring mechanisms to ensure robust protection against endpoint-based threats.

22. Vendor Risk Management Audits – Assessment of third-party and vendor cybersecurity practices to identify supply chain risks and ensure alignment with organizational security policies.

23. Evaluation of SBOM – Software Bill of Materials to ensure transparency, traceability, and integrity of components used in software systems. This audit focuses on identifying known open-

source and third-party components, and verifies adherence to secure development lifecycle practices and regulatory compliance.

3.2.3 Audit of Identity and Access Management (IAM):

1. Audit of the access control policies to check the implementation of authentication, authorization, role-based access control, segregation of duties, and least privilege principles.
2. Assessment of password policies and effectiveness of its implementation.
3. Assessment of the implementation of Multi Factor Authentication for critical systems.
4. Audit of defined remote access policies and implemented cybersecurity measures by the utility for remote access cybersecurity.
5. Audit of mobile device policies, addressing cybersecurity risks associated with use of external removable and BYOD systems as defined in cybersecurity policy.

3.2.4 Application and Data Security

1. Audit of the process for data classification based on sensitivity and criticality.
2. Audit to check the implementation of data retention, data access controls, and data leakage prevention mechanism. This includes audit of the mechanism/ system used for data encryption to evaluate their effectiveness in protecting sensitive data, both at rest and in transit.
3. Audit to check the effectiveness of data backup strategies and the ability to recover from data loss or corruption.
4. Audit of Cryptographic controls, key management, and key storage mechanism (if in use).
5. Audit of the practices used or followed for In-house or Out-sourced application development, secured coding practices and code testing process.
6. Audit to check implementation of data security and data privacy measures to ensure compliance with applicable rules and regulations for protection of sensitive data.
7. Audit the cybersecurity mechanisms deployed in the database to identify potential threats and ensure the protection of sensitive information.
8. Evaluation of the measures in place for data protection in cloud environments, including backup and encryption.
9. Review of the security practices of cloud service providers and any third-party integrations as per standards.

3.2.5 Logging and Monitoring

1. Audit of the mechanism/system in place to monitor, detect and log events of deployed security devices, networks, end devices and hosts.
2. Review of the logs storage systems in place to comply with existing regulatory requirements. This includes review of the operational and functional efficacy of the Security Operational Centre (SOC) to check for threat detection and response capabilities.
3. Review of the deployment and effectiveness of logging and monitoring solutions, such as SIEM, to ensure timely detection and response to security incidents.
4. Log Management and Maintenance Audit-Assessing the effectiveness and completeness of system and security log generation, retention, integrity, and monitoring practices, ensuring that logs are maintained in accordance with organizational policies and regulatory requirements to support detection, investigation, and response activities.

3.2.6 Audit of Incident Management Process

1. Audit of the incident response process and customization for the power sector, and its effectiveness across IT, OT and IoT systems.
2. Evaluation of the effectiveness of the deployed tools and processes for detecting and monitoring of the cybersecurity incidents.
3. Audit of procedures for identifying and reporting security incidents.
4. Review of previous audit/ Incident Report (IR) reports and their compliance status.
5. Assessment of the processes for conducting post-incident reviews and implementing lessons learned.

3.2.7 Audit of the Architecture, Networks and Systems

1. Audit of the IT, OT and IoT System as-built Architecture for Assessment of Structural Weaknesses, Interconnections, Data Flow, Communication Protocols, and System Convergence and identification of gap.
2. Review of the deployment of appropriate perimeter security devices, Security of trusted zones & conduits, network segmentation, and IT/OT convergence.
3. Audit to check the security configurations of servers, workstations, and other endpoints and to verify the deployment of Endpoint Security solutions such as Antivirus, EDR solutions.
4. Audit of configurations of security devices, host devices and network devices configurations and to review implementation of required hardening measures such Blocking of unnecessary ports and

services, whitelisting of applications, and others in comparison with cybersecurity benchmarks like CIS Benchmarks.

5. Audit of standard operating procedure for configuration management of systems and devices.
6. Review of DC / DR Systems - Review of security Architectures of Main / Backup sites, their interconnections, and data flow.

3.2.8 Audit of Physical Security

1. Audit of physical Access controls to evaluate the effectiveness of physical access controls and surveillance systems, visitor management, and employee identification systems.
2. Review of logs and records of physical access and Comparison of physical security measures with industry standards and best practices.
3. Audit of the mechanism/system in place for Protection from physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure.

3.2.9 Audit to Check Conformance and Compliance

1. Cybersecurity Audit of IT, OT and IoT Infrastructure to check conformance with utility Cybersecurity Policy.
2. Verification audit to check compliance with applicable Cybersecurity rules, regulations, directives, and guidelines issued by CERT-In, NCIIPC, Ministry of Power and other relevant Authority.
3. Verification Audit to check utility cybersecurity program alignment with cybersecurity standards and best practices such as ISO 27001, ISO 27019, IS 16335, IEC 62443 series standards as applicable.
4. Verification Audit to check compliance with Cyber Security Audit - Baseline Requirements (CSA-BR) 2020, issued by the NSCS.
5. Verification Audit to check compliance with NCRF document, issued by the NCIIPC/CEA.
6. Verification of: - Retention of valid FAT/SAT and conformance test certificates for in-service OT/IoT equipment. - IEC 62443-4 self-declaration or certification for equipment from non-Trusted Sources. - Embedding of Trusted Source / certification requirements in future procurement processes.

3.2.10 Audit Deliverables

1. Detailed plan outlining objectives, scope, methodology and timeline.

2. Auditor should immediately inform the critical findings observed (if any) during audit to BESCOM for their immediate action.
3. Gap analysis report with respect to framework and architecture
4. Suggestions and recommendations to address audit findings.
5. Suggestion for having secure network architecture.
6. A roadmap for implementing recommended security measures and improvements.
7. Schedule of follow-up audits to verify the implementation of corrective actions.
8. Identified gap and Suggestion to update cybersecurity policies, procedures, and controls based on audit findings and evolving threats.
9. The audit report shall provide a comprehensive and detailed account of the entire audit process. It should include identified vulnerabilities, risks, non-compliance issues, with artefacts and evidence and areas for improvement.
10. The audit report should also encompass the audit mechanism, detailed scope, duration, methodologies, standards used, tools, manual processes, findings, prioritization, sampling decisions, manpower involved, as well as any exemptions, limitations, and other constraints encountered during the audit. Additionally, a list of the testing software or tools used should be included.
11. The report should begin with an executive summary that offers a concise overview of the audit findings, highlighting the associated risks to the organization and the overall security posture of the audited application or infrastructure. This summary is intended for submission to higher management, including board members.
12. Exit briefing: Convey preliminary interim audit observations to BESCOM, such as critical findings, vulnerabilities, major gaps etc. which require immediate attention / action and educating the utility in providing feedback to the empaneling agency about the quality of the audit performed by empaneled auditors at utility end.
13. All audit observations, findings and recommendations shall be supported by verifiable technical evidence. Such evidence shall include but not be limited to system logs, configuration files, screenshots, tool outputs, network traces and access records.
14. No observation shall be accepted without supporting artefacts. BESCOM reserves the right to seek additional proof or validation for any reported finding.
15. Auditors are required to implement both CVSS and Exploit Prediction Scoring System (EPSS) frameworks within their audit

reports. The observations/vulnerabilities in the report must be categorized based on the Common Vulnerability Scoring System (CVSS) for severity and supplemented with the Exploit Prediction Scoring System (EPSS) to assess the likelihood of real-world exploitation.

3.3 Part 2 Guideline on the Scope of Vulnerability Assessment (VA) & Penetration Testing (PT)

This guideline outlines the scope, activities, methodology and deliverables for conducting a Vulnerability Assessment (VA) & Penetration Testing (PT) audit. Part-2 should be implemented in conjunction with Part-I for a comprehensive cybersecurity audit.

Vulnerability Assessment/Penetration Testing (VA/PT)

1. Vulnerability analysis of all notified Protected Systems, critical and high-risk assets. Medium and low-risk assets should be covered on a sample and rotation basis.
2. VA/PT of web applications, web-based services, mobile applications, on cloud hosted applications, IoT applications, other publicly exposed services including assessment of security architecture and design review of these applications.

Special Considerations for VA/PT of OT Systems

1. In OT systems, where active Vulnerability Assessment (VA) and Penetration Testing (PT) may not be feasible, VA should be conducted in passive mode or through physical verification to avoid disruptions to critical processes. The use of passive scanning tools that do not actively interact with OT devices should be ensured.
2. Active Vulnerability Assessments and Penetration Testing may be conducted in simulated environments or isolated test setups. Additionally, targeted testing should be performed on testbeds or during planned maintenance windows to assess system vulnerabilities. In latter case, the target OT systems and their components should be clearly identified to minimize operational impact. Components that cannot tolerate downtime or interruptions should be excluded from testing.

3.3.1 Scope of work

The scope of work should include conducting comprehensive Vulnerability Assessment and Penetration Testing (VA/PT) as defined, documenting and reporting identified vulnerabilities and cybersecurity issues, supporting the remediation and closure of identified gaps and

ensuring compliance with VA/PT requirements in alignment with security standards and best practices.

It should include the following:

1. Assessment of systems and networks of identified Critical Information Infrastructures (CII), notified Protected Systems, critical and high-risk systems including servers, virtual machines, software applications, workstations, and other endpoint devices.

2. Assessment of systems and networks segment having medium and low risk cyber assets in sample and rotation basis.

3. Vulnerability assessment and penetration testing (VA/PT) of web applications, mobile applications, cloud-based applications, APIs, in-house-developed applications and other internal applications.

4. Assessment of network architecture and data flow within IT, OT and IoT environments for structural weaknesses, interconnections, communication protocols, data flow, and system convergence.

5. Assessment of security configurations for deployed devices, including firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), routers, switches, and other network devices.

6. Assessment of perimeter security devices and network including testing for potential exploitations from outside.

3.3.2 Vulnerability Assessment (VA)

Objective is systematic examination of IT, OT & IoT system, web and mobile applications or product to identify security deficiencies, determine the adequacy of security measures, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

3.3.2.1 Activities

The vulnerability assessment should cover a range of activities to identify security weaknesses, the list of sample activities to is mentioned below:

1. Port and Network Scanning: Identify open ports and services running on the network.

2. Vulnerability Scanning: Use automated tools to detect vulnerabilities across all systems in scope.

3. System and Service Identification: Enumerate and fingerprint operating systems and services.

4. Malware Scanning: Detect and analyze any malware or potential threats

within the network.

5. Password Strength Assessment: Assessment of the strength of passwords.

6. Authentication and Authorization Testing: Test access control mechanisms and account lockout policies.

7. Configuration Assessment: Assessment of network devices configuration such as firewall configurations for security gaps.

8. Server and Database Assessment: Evaluate OS and database configurations for vulnerabilities.

9. Any additional activities as mutually agreed upon by BESCOM and the auditor.

10. Wireless Security Testing- Evaluating the security measures of a wireless network by simulating attacks to identify potential vulnerabilities and ensure the network is protected against unauthorized access and data breaches.

3.3.2.2 Methodology

1. Preparation – Determine the boundaries for analysis
2. Execution - Conduct assessments using both automated tools and manual techniques, as applicable.
3. Analysis - Analyze the results to identify the vulnerabilities and security gaps
4. Reporting - Document findings, categorize vulnerabilities by risk level and provide remediation recommendations.
5. Validation - Perform a validation assessment to confirm the resolution of identified vulnerabilities.

3.3.2.3 Deliverables

The vulnerability assessment should systematically identify security vulnerabilities, provide actionable steps for remediation and outline a plan to enhance the overall security posture. The deliverables may include the following:

1. Vulnerability Assessment Report having

a. detailed Findings of identified vulnerabilities, including their severity, potential impact, and affected systems or applications.
b. categorization of vulnerabilities by risk level (e.g., Critical, High, Medium, Low).
c. assessment of the potential impact of the vulnerabilities on the system and operations of the utility.
d. technical documentation with scan results and screen shots supporting the identified vulnerabilities.

e. Vulnerability, Threat, Risk assessment report based on the KPIs as per CEA/CERT-In/MoP/NCIIPC guidelines.

2. Remediation Plan outlining

a. the steps necessary to close identified vulnerabilities, including any required patches or configuration changes.

b. comparison of current security posture against industry benchmarks and standards.

c. plan for overall improvement of the cybersecurity posture by adherence to relevant security standards and best practices.

3.3.3 Penetration Testing:

The objective is to simulate real-world attacks to identify methods for bypassing the security features of the utility's applications, systems, or networks. Assessors, operating under defined constraints, attempt to exploit or circumvent these security measures. Most penetration tests involve discovering and exploiting combinations of vulnerabilities across one or multiple systems to achieve broader access than would be possible through a single vulnerability alone.

3.3.3.1 Internal Penetration Testing (PT)

Internal Penetration Testing may be conducted to simulate an insider attack for identification of potential vulnerabilities within the internal network and applications.

Internal Penetration Testing should cover:

1. Network Infrastructure: Routers, switches, firewalls and security appliances within the internal network.

2. Servers and Workstations: Internal-facing servers, desktops, and other endpoints.

3. Applications: Internal web and client-server applications.

4. Any additional systems or products as specified within the scope.

a. Activities:

A list of sample activity for Internal Penetration Testing may include:

1. Port Scanning and System Enumeration: Identify open ports, running services, and system details.

2. Security Bypass: Attempt to bypass security controls such as EDR, firewalls and intrusion detection/prevention systems (IDS/IPS).

3. Privilege Escalation: Test for potential paths to escalate privileges within the network.

4.Exploitation of Vulnerabilities: Attempt to exploit identified vulnerabilities to assess their impact.

5. Lateral Movement: Evaluate the ability to move laterally within the network after initial compromise.

6. Data Exfiltration: Simulate data exfiltration scenarios to test data security.

b. Methodology:

1. Pre-engagement: Agree on the rules of engagement, define the testing scope, objectives, and constraints in consultation with the utility. Identification of key systems, networks, and applications to be tested.

2. Reconnaissance: Gathering the information about the internal network, systems, and users to identify potential targets and vulnerabilities.

3. Vulnerability Identification: vulnerability scanning to identify security weaknesses within the internal environment.

4. Exploitation: Attempting to exploit identified vulnerabilities to gain unauthorized access, escalate privileges, or move laterally within the network.

5. Post-Exploitation: Assessment of the potential impact of successful exploitation, including access to sensitive data, disruption of services, or compromise of critical systems.

6. Reporting: Detailed findings, including exploited vulnerabilities, impact analysis, and remediation recommendations.

c. Deliverables:

Penetration Testing Report: A comprehensive report detailing the tests performed, vulnerabilities exploited, and the impact on the organization.

Mitigation Strategies: Recommendations to mitigate identified risks, including policy updates and system configuration changes.

3.3.3.2 External Penetration Testing:

To assess the organization's exposure to external threats by simulating real-world attacks against public-facing infrastructure.

a. Scope

The external PT covers:

i. Public-Facing IPs: All external IP addresses exposed to the internet.

ii. Web Applications: Web applications and Mobile applications accessible via the internet.

iii. Firewall and Security Devices: External security devices such as firewalls and IDS/IPS systems.

b. Activities

Testing will include:

i. Reconnaissance: Gather information about the target network and its public IPs.

ii. Port Scanning: Identify open ports and services on public-facing systems.

iii. Vulnerability Exploitation: Attempt to exploit known vulnerabilities in public-facing systems.

iv. Attack Simulation: Simulate various attacks such as SQL injection, cross-site scripting (XSS), and remote code execution (RCE).

v. Denial of Service (DoS) Testing: Simulate DoS attacks to assess system resilience. DoS resilience assessment through controlled simulation or non-disruptive methods.

vi. Firewall and IDS/IPS Testing: Assess the effectiveness of perimeter defenses.

c. Methodology

i. Preparation: Define the scope, identify public-facing assets, and establish testing windows.

ii. Testing: Conduct external penetration tests using both manual techniques and automated tools.

iii. Analysis: Analyze test results to identify vulnerabilities and potential

security risks.

iv. Reporting: Document all findings and provide recommendations for improving external security.

d. Deliverables:

i. External Penetration Testing Report: A detailed report of the findings with recommendations for mitigating risks.

ii. Security Improvement Plan: A plan outlining steps to enhance the security posture of external-facing systems.

3.3.4 Website/Web Application Assessment

To ensure the security of web applications through a detailed assessment of their security posture. The OWASP guidelines may be used.

a. Scope

This should include:

i. Web and Mobile Applications: All publicly exposed web-based and mobile applications.

ii. APIs: Application Programming Interfaces (APIs) associated with the web applications.

b. Activities

The assessment will focus on:
i. Input Validation: Test for vulnerabilities such as SQL injection, cross-site scripting, and input validation flaws.
ii. Authentication and Session Management: Assess the security of authentication mechanisms and session management.
iii. Access Control: Test the effectiveness of access control measures.
iv. Security Misconfigurations: Identify misconfigurations that could lead to vulnerabilities.
v. Data Exposure: Test for sensitive data exposure and improper data handling.
vi. API Security: Assess the security of APIs associated with the web applications.

c. Methodology

i. Black Box Testing: Conduct testing without prior knowledge of the internal workings of the application.

ii. Gray Box Testing: Combine black box testing with some knowledge

of the application's internals.

iii. Manual and Automated Testing: Use a combination of automated tools and manual techniques to identify vulnerabilities.

d. Deliverables

i. Web Application Security Report: A report detailing identified vulnerabilities, risk levels, and recommended mitigations.

ii. Compliance Check: Ensure that the application complies with relevant security standards such as OWASP Top Ten.

3.3.5 Resolution, Compliance, and closure of Cybersecurity Vulnerabilities

Objective- To ensure that identified vulnerabilities are properly closed and that the compliance with the requirements

a. Scope

i. Vulnerability Closure: Suggestions and technical recommendations to close identified vulnerabilities including patches and configuration changes. Need to ensure that remediation timelines are aligned with applicable regulatory requirements. All Critical and High vulnerabilities shall be remediated within a period of one (1) month from identification, and Medium and Low vulnerabilities shall be remediated before the commencement of the next audit cycle.

Closure of vulnerabilities shall be verified through re-testing and documented evidence

ii. Compliance Assurance: Ensure that all remediation activities align with power sector requirements and relevant standards.

b. Deliverables

i. Remediation Report: A report detailing the remediation efforts and verifying the closure of identified vulnerabilities.

ii. Compliance Documentation: Documentation to support compliance as required by the utility.

3.3.6 Re-Scan

Objective -To verify that previously identified vulnerabilities have been effectively remediated.

a. Scope

Re-Scan Activities: Conduct a follow-up assessment to confirm that all identified vulnerabilities have been resolved.

Validation: Validate the effectiveness of the remediation efforts through a comprehensive re-scan.

Re-Scan Report: A report confirming the closure of vulnerabilities and the overall improvement in security posture.

3.3.7 <u>Cyber Forensic Assessment:</u>

a. Must carry below assessments at Data center, end-devices and network (wherever applicable) in case of any cyber incident reported by BESCOM
   - Assessment and threat hunt on the end-point devices (by visiting remote offices).
   - Compromise Assessment
   - System/Data exposure assessment
   - Data flow channel assessment
   - In-depth network Monitoring and inbound / outbound traffic analysis
   - Agent based framework to take responsive actions
   - Orchestration
   - Automated Continuous Threat hunting to look for any trace(s) of APT executions
   - Threat Intelligence Based Monitoring
b. To analyze and report about breach identified (if any) on a specific end point
c. Identify any Malicious activity including but not limited to, Botnet activity, Command & Control activity
d. Provide Fact Finding Report on completion of Assessment
e. Identify and report remediation recommendations.
f. All observations must be supported with verifiable technical evidence such as logs, screenshots, configurations and tool outputs

3.3.8 The cybersecurity audit shall include a comprehensive Source Code Security Review for applications where source code access is available.

The source code review shall be conducted using a combination of automated Static Application Security Testing (SAST) tools and manual secure code review techniques.

The review shall assess application code against secure coding standards and identify vulnerabilities including but not limited to:

- Input validation flaws, injection vulnerabilities and insecure data handling

- Authentication and authorization weaknesses
- Improper session management
- Cryptographic implementation issues
- Hardcoded credentials, secrets and keys
- Business logic flaws and insecure workflows

The assessment shall align with industry best practices such as OWASP secure coding guidelines and OWASP Top 10 vulnerabilities.

The bidder shall provide a detailed Source Code Review Report including identified vulnerabilities, severity classification, affected modules and actionable remediation recommendations.

In cases where source code is not available, the bidder shall explicitly document the limitation and ensure enhanced black-box and grey-box testing coverage for such applications.

3.3.9 IoT & Field Device Cyber Security Audit Scope:

In addition to IT and OT systems, the audit shall include detailed cybersecurity assessment of IoT and field devices such as Smart Meters (AMI), RTUs, PLCs, AMR meters, communication modules, and field gateways.

Audit shall include end-to-end AMI system covering device, communication, Head End System (HES) and Meter Data Management (MDM).

Protocol-level VAPT shall be conducted for all applicable OT and IoT communication protocols including IEC 62056 (Device Language Message Specification & Companion Specification for Energy Metering), IEC 60870-5-104, Modbus, DNP3 and IEC 61850. The assessment shall include validation of authentication mechanisms, encryption, secure session management, and key management as per IEC 62351, along with testing for plaintext communication, unauthorized command injection, replay attacks, protocol fuzzing, man-in-the-middle and denial-of-service scenarios. The audit shall further evaluate implementation of network segmentation, zones and conduits, and defence-in-depth architecture in alignment with IEC 62443 standards and NIST SP 800-82.

3.3.10 Implementation Timelines:

The schedule for completion of tasks for is as mentioned below:

Sl No	**DELIVERABLE**	**Timeline** **('T' – date of issue of contract order)**

1	Approach document for Cyber security Audit (part-1 of this scope) and VAPT (part-2 of this scope) for all IT/OT/IoT systems, web and mobile applications of BESCOM.	T + Week 1
2	Deployment of Team for performing cyber security audit and VAPT for communication with BESCOM.	T + Week 1
3 (*)	Report on findings of Cyber security audit (part-1 of this scope), VAPT (part-2 of this scope) performed on BESCOMs IT/OT/IoT systems, web and mobile applications along with proposed remediation Action.	T+ Week 10
4	Final Report of systems per assessment activity with Remediation's and Recommendations shall be submitted to BESCOM.	On or before T+ Week 13
5	Debrief of Executive Summary and Lessons learnt after completion of each assessment activity with BESCOM Management & submission of final Reports with recommendations and Presentation for any clarifications.	On or before T+ Week 14 (or as intimated by BESCOM)

(*) In case of any Critical/High vulnerabilities identified in the systems during assessment activity, such vulnerabilities to be reported to BESCOM immediately to patch the vulnerabilities on time.

Note: The above table is applicable for each and every cycle of audit activity.

4 General

a. This EOI is issued only to discover the market price from eligible bidders to perform the Cyber Security audit activity in BESCOM.

b. Bidder may seek clarifications related to this EOI within the timeframe specified in KPP portal.

c. Bidder shall not disclose or use such information for purposes other than participation in this EOI.

d. General Conditions of Expression of Interest (EOI):

- Bidder shall be a registered Company/Partnership/LLP/Proprietorship in India.
- Entities blacklisted or debarred by any Government/PSU are not eligible.
- Bidder must be an empaneled service provider by CERT-IN as Information Security Audit Organization.
- The Bidder shall have a. ISO 9001:2015 or latest certification and b. ISO 27001:2022 or latest certification
- The bidder shall have minimum experience of 5 years in performing Cyber Security Audit project in any of the Central/State Government, Undertaking Electrical Utility, Government bodies / Public /Private sector in India i.e., during the last five Financial Years (2021-22, 2022-2023, 2023-2024, 2024-2025 and 2025-26)

e. EOIs shall not be considered in case of:
   - Incomplete or non-compliant submissions
   - Misrepresentation of facts
   - Conflict of interest
   - Submission after the deadline
   - Abnormal/subnormal quotes

f. Confidentiality: All information provided by the Tender inviting authority must be treated as confidential. BESCOM may at its own discretion may use the price discovered from the EOI for any projects/works/activities/tenders.
g. Issuance of this EOI does not constitute a commitment to award or proceed with procurement.
h. This EOI is published only to arrive at the amount put to tender (APT) for the notified scope of work. There will not be any contractual obligations and no Contract award will be given.
i. Breakup of prices shall be provided upon request from BESCOM for the quoted price in EOI.
j. Validity: Price quoted shall remain valid for a period of 180 days from the date of submission of this EOI.
k. Right to Reject: EOI inviting authority reserves the right to reject any or all EOIs without providing reasons.
l. This EOI shall be cancelled after discovering price without any further notice.

5 Particulars:

The cyber security audit scope for BESCOM includes assessment of multiple IT, OT and IoT systems, web and mobile applications of varying size and complexity, comprising large, medium and small-scale systems. The applications include critical infrastructure systems such as IPDS, ERP and TRM System categorized as large applications; medium-scale systems such as Prepaid Metering; and several small-scale applications including web portals,

mobile applications, financial systems, GST software, EV portal, SRTPV system and field devices like spot billing systems. OT system- Distribution Automation System (DAS) and IoT system- AMI (Advanced Metering Infrastructure) System

Bidders are required to consider the diversity, criticality, and complexity of these applications while estimating the effort and costing for conducting cyber security audit as per the scope defined in this document.

Note- The mentioned classification of applications is indicative in nature.

5.1 The applications in BESCOM are categorized as below:

TABLE 1: For IT applications only

SL No	Type of application	Classification details
1	Large Application	**Large Application with respect to VAPT and Security audit:** 1. On-Premises & Cloud Both 2. Availability of DC & DRC 3. OS type – Windows & Linux Both 4. OS Version – Lower & multiple 5. API Integration more than 1000 6. Static IP Address: >10 7. Servers count more than 100 8. Application User: Internal User and External User 9. Virtualization & Physical Server Both 10. Data Flow among Modules complexes 11. Data Input Source: Multiple 12. Framework Version: lower and Multiple 13. Database type: Multiple (Oracle, MS SQL, MySql, etc.) 14. Database version: lower & Multiple 15. Database Accessibility: Admin and Multiple other users 16. Web Based Application & Mobility Solution (Android & iOS) Both 17. Accessibility Authentication: Multi factor 18. Source Code available: yes 19. Application Accessibility: Web based & SSH & Telnet 20. VAPT Expertise Requirement: High 21. VAPT Duration: 10 Days and Above Example : Large applications like IPDS, TRM, ERP and miscellaneous

2	Medium Application	**Medium Application with respect to VAPT and Security audit:** 1. On-Premises OR Cloud 2. Availability of DC Only 3. OS type – Windows / Linux / Both 4. OS Version – Lower & multiple 5. API Integration more than 500 6. Static IP Address: 5-10 7. Servers count 50-100 8. Application User: Internal User OR External User 9. Virtualization OR Physical Server 10. Data Flow among Modules: medium complex 11. Data Input Source: Multiple 12. Framework Version: lower and Multiple 13. Database type: Single (Oracle, MS SQL, MySql, etc.) 14. Database version: lower OR Multiple 15. Database Accessibility: Admin and few other users 16. Web Based Application OR Mobility Solution (Android & iOS) 17. Accessibility Authentication: Password based 18. Source Code available: yes 19. Application Accessibility: Web based OR SSH OR Telnet 20. VAPT Expertise Requirement: Medium 21. VAPT Duration: 5 -10 Days Example : Medium scale applications like Pre-paid meters and miscellaneous
3	Small Application	**Small Application with respect to VAPT and Security audit:** 1. On-Premises OR Cloud 2. Availability of DC Only 3. OS type – Windows / Linux 4. OS Version – Latest OR N-1 5. API Integration less than 100 6. Static IP Address: 2-5 7. Servers count less than 50 8. Application User: Internal User 9. Virtualization OR Physical Server 10. Data Flow among Modules: less complex 11. Data Input Source: Few 12. Framework Version: Latest or N-1 13. Database type: Single (Oracle, MS SQL, MySql, etc.) 14. Database version: Latest OR N-1 15. Database Accessibility: Admin only 16. Web Based Application OR Mobility Solution (Android & iOS) 17. Accessibility Authentication: Password based 18. Source Code available: yes 19. Application Accessibility: Web based 20. VAPT Expertise Requirement: Low 21. VAPT Duration: 2- 5 Days Example : Small scale applications like SBM, BESCOM official website, Financial accounting systems, Finance and accounts Management software (cash management), GST software, EV web, mobile app, Jagruthi portal,Ganagakalyana web app, HT Mithra, BESCOM Mithra and miscellaneous

TABLE 2: For OT system:

Sl No	Type	Classification Details
1	OT System	1. SCADA+DMS + RTU + IT integration 2. Field devices may include RTUs, IEDs, PLCs, protection relays and gateways. 3. Protocols: IEC 60870-5-104, DNP3, Modbus, IEC 61850 4. Multi-vendor OEM environment 5. Integrated with enterprise IT systems 6. Wide-area / utility-scale deployment 7. High grid operational criticality 8. Real-time monitoring and control systems 9. Requires sampling-based device testing 10. Protocol-level VAPT required 11. Compliance: IEC 62443 + IEC 62351 12. Secure architecture validation (zones & conduits) 13. Hybrid communication infrastructure (Fiber/RF/Cellular) 14. Validation of control commands (open/close operations) to prevent unauthorized switching actions 15. VAPT duration: 10–15 days

TABLE 3: For IoT systems

Sl No	Type	Classification Details
1	IoT System	1. Smart meters (AMI enabled field meters) 2. Components: Meter + DCU + HES + MDM 3. Protocol: DLMS/COSEM + IEC 62056 4.End-to-end AMI architecture covering meter → DCU → HES → MDM 4. Multiple OEMs & firmware versions 5. Integrated with billing/IT systems 6. Wide geographic deployment 7. Sampling-based VAPT mandatory 8. Communication tech: RF/GPRS/NB-IoT 9. Key mgmt. & encryption validation 10. Protocol-level assessment of DLMS/COSEM communication security 11. VAPT duration: 10–12 days

5.2 The bidders are informed to provide the market rates (inclusive of all applicable taxes) in the below format keeping the above tables (TABLE 1, TABLE 2 and TABLE 3) as reference by considering the entire Scope of work mentioned in Section 3 (separate rates for part 1 and part 2 of the scope) of this document. The bidder shall consider variability in the number, size, complexity, and criticality of applications and systems while quoting.

No additional cost shall be claimed due to variations in architecture complexity within the defined classification (Large/Medium/Small).

TABLE-4

PART 1					
SL No.	**Description**	**Extent of Contract (A)**	**Qty (B)**	**Unit Rate (in Rs.) (inclusive of all applicable taxes) (C)**	**Total In Rs. (inclusive of all applicable taxes) (B*C)**
1	Comprehensive Cyber Security Audit of all BESCOM IT/OT/IoT Systems, Web Applications, Mobile Applications, Policies, Processes, Governance Structure and Compliance Requirements as per Scope defined in Part-1	yearly - one no. of audit cycle to be performed in one year	1		

PART 2					
SL No.	**Description**	**Extent of Contract (A)**	**Qty (B)**	**Unit Rate (in Rs.) (inclusive of all applicable taxes) (C)**	**Total In Rs. (inclusive of all applicable taxes) (B*C)**
2	Vulnerability Assessment & Penetration Testing (VAPT) of IT Application -	Yearly – two nos. of audit cycles for each application to be performed in one year (2	4 applications		

	Large (Large applications like IPDS, TRM, ERP and miscellaneous)	cycles each/year)			
3	Vulnerability Assessment & Penetration Testing (VAPT) of IT Application - **Medium** (Medium scale applications like Pre-paid meters and miscellaneous)	Yearly – two nos. of audit cycles for each application to be performed in one year (2 cycles each/year)	2 applications		
4	Vulnerability Assessment & Penetration Testing (VAPT) of IT Application - **Small** (Small scale applications like SBM, BESCOM official website, Financial accounting systems, Finance and accounts Management software (cash management), GST software, EV (web & mobile app, Jagruthi portal), GangaKalyana web app, HT Mithra mobile app, BESCOM Mithra mobile app and miscellaneous)	Yearly – two nos. of audit cycles for each application to be performed in one year (2 cycles each/year)	10 applications		
5	Vulnerability Assessment & Penetration Testing (VAPT) of IT Application of DAS system(IT Application	yearly - one no. of audit cycle for DAS application to be performed in one year	1 application		

	(classified as Large Scale) along with OT Assessment including 10 sampled RTUs)				
6	Vulnerability Assessment & Penetration Testing (VAPT) of IT Application AMI System (IT application (classified as Medium scale) + IoT system including 16 nos. of sampled meters)	Yearly – two nos. of audit cycles to be performed in one year	1 application		
Total (Part-2)					
Total Amount put to tender (Part-1 + Part-2) Inclusive of all taxes in Rs.					

5.3 The quantity of assets, systems, devices, applications, interfaces, APIs, servers, field devices, communication links and other components provided for assessment under each application/system may vary during actual execution. In case BESCOM provides only partial scope/assets for assessment against a particular application/system, the payment shall be made on a pro-rata basis corresponding to the actual percentage/quantity of assets assessed, duly certified by BESCOM.

5.4 The quantity of field devices, smart meters, RTUs, IEDs, PLCs, protocols, communication links and sampled assets may vary during actual execution. BESCOM reserves the right to decide the sample size, coverage and final assessment scope during each audit cycle.

5.5 Sampling percentage and selection criteria for OT and IoT field devices shall be decided by BESCOM based on criticality, geography, OEM diversity, firmware versions, communication technologies and operational constraints. BESCOM may include different makes, models, firmware versions and OEMs during assessment activities

5.6 Bidders shall strictly quote only in the above format. Any deviation or lump sum pricing shall be rejected.

5.7 Other general requirements (no separate costing will be provided for the below):

- The bidder shall strictly adhere to leading practices of project execution. Assess and evaluate cyber security requirements considering the management interests, goals, objectives, risk tolerance and other strategic objectives of BESCOM.
- The bidder shall arrange a weekly progress meeting with BESCOM to share the completed task and in progress items.
- The bidder shall deploy dedicated Cyber Security audit, VAPT, Network Analysis & Cyber Forensics resources to be stationed onsite at BESCOM during the audit activity (part-1 and part-2).
- Daily critical observations shall be reported to BESCOM SPOC.
- Detailed weekly report to be sent to BESCOM SPOC.
- Final Assurance Report to be provided on closure of each engagement.
- Bidder shall provide logs of assessment tool execution.
- Bidder shall ensure that the assessment tests carried out during Cyber security audit and the testing approach comply with the guidelines issued by CERT-In and industry standard practices. A detailed report indicating the tests & checks that will be carried along with tools & processes shall be shared with BESCOM for acceptance within the 1st week from the date of issue of DWA.
- Tools used shall be industry-recognized and capable of identifying OWASP Top 10, CVEs and misconfigurations aligned with CIS benchmarks also.
- The tools used shall support both automated and manual validation techniques. BESCOM reserves the right to review and approve the tools prior to commencement of the audit.
- BESCOM reserves the right to evaluate the quality of audit performed by the bidder based on accuracy, completeness, technical depth and evidence provided.
- In case of inadequate, incomplete, or superficial audit findings, BESCOM reserves the right to reject the report and require re-assessment at no additional cost.
- Bidder shall adhere to the CEA (Cyber Security in Power Sector) Guideline, 2021, Article 14. Cyber Security Audit and Information Technology Act, 2000, to perform Cyber Security Audit of IT/OT/IoT systems, web applications and mobile applications in BESCOM. The compliance to the same has to be provided to BESCOM.
- The Bidder shall facilitate and co-ordinate with concerned stakeholders of IT/OT/IoT systems of BESCOM for the pre-requisites to perform Cyber security audit by themselves.
- The successful bidder has to provide Key professionals such as Team leader (1 no.) with 8-10 yrs working experience, Engineer with VAPT expertise (4 nos.) with 5-8 yrs working experience, Engineer with Cyber Forensic expertise (2 nos.) with 5-8 yrs and Engineer with Cyber security audit expertise (3 nos.) with 5-8 working experience in the field of performing VAPT, Cyber Forensic and cyber security audit with Core expertise.

- The CVs recently signed in blue/black ink by the respective Personnel and countersigned by the Applicant shall be submitted by successful bidder. Photocopy or unsigned/countersigned CVs shall be rejected.
- Any replacement of the existing resource during the Contract Period can be done only by a person of similar/higher experience and qualification and in agreement with the utility.
- The successful bidder shall make their own arrangements of hardware and Internet Facility required for performing VAPT, Cyber Forensic Assessment and cyber security audit of IT/OT/IoT systems, web and mobile applications of BESCOM.
- Variation clause-The number of IT/OT/IoT systems, web and mobile applications provided by BESCOM for the particular cycle of cyber security audit will be final which may include addition/omission of the applications for the Cyber Security Audit activity list given at the initial stage. The payment will be made on the basis of number of IT/OT/IoT systems, web & mobile applications audited.
- The successful bidder should coordinate with the concerned Stakeholders of BESCOM during VAPT, Network Analysis and Cyber Forensic Assessment of IT/OT/IoT systems, web and mobile applications provided by BESCOM in order to mitigate the vulnerabilities identified.
- The tools/platform used for performing VAPT, Cyber Forensic Assessment and Cyber security audit should be compatible with the BESCOMs IT/OT/IoT systems.
- The successful bidder has to use the licenced tools to perform VAPT, Cyber Forensic Assessment and cyber security audit. The licence details has to be shared with BESCOM prior to performing the assessment. No additional cost will be paid to the tools used to perform any kind of activity separately, it's all inclusive for part-1 and part-2 of the scope of work.
- Non-Disclosure Agreement (NDA) for Data sharing as per the Data Sharing Policy of BESCOM version 2 should be executed between BESCOM and all the team members having access to BESCOMs IT/OT/IoT systems, web and mobile applications.
- Upon completion of the assessment activity the successful bidder should certify stating that the data shared by BESCOM/ reports of the assessment provided by the successful bidder shall be kept confidential.

*****